WHAT IS CLAIMED IS:

1. A computer readable medium containing a database structure for storage of encrypted data, the database structure comprising:

at least one data entity encrypted by at least one encryption key, the data entity having at least one searchable attribute; and

at least one encryption key identification in association with the data entity and corresponding to the encryption key.

2. The computer readable medium according to claim 1 wherein the at least one encryption key identification is encrypted by a system key, and the database structure further comprises a system key common name corresponding to the system key, and the system key common name being stored in association with the data entity.

3. The computer readable medium according to claim 2 wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name.

4. The computer readable medium according to claim 3 wherein the system key common name and the system key common name hash value are stored on a separate database from the at least one data entity.

5. The computer readable medium according to claim 1 wherein the at least one encryption key identification is encrypted by a system key.

6. The computer readable medium according to claim 1 wherein the at least one encryption key comprises a dynamic encryption key, and the at least one encryption key identification comprises a dynamic encryption key identification.

7. The computer readable medium according to claim 1 further comprising a plurality of data entities encrypted by a plurality of encryption keys, and a plurality of encryption key identifications.

8. The computer readable medium according to claim 7 wherein the plurality of encryption keys comprise dynamic encryption keys, and the plurality of encryption key identifications comprise dynamic encryption key identifications.

9. The computer readable medium according to claim 1 wherein the data structure further comprises a plurality of hash values with each of the searchable attributes having a corresponding hash value.

10. The computer readable medium according to claim 1 wherein the data structure further comprises at least one integrity attribute in association with the data entity.

11. The computer readable medium according to claim 1 wherein the data structure further comprises a security key attribute of the data entity, the security key attribute including the at least one encryption key identification and a system key common name.

12. The computer readable medium according to claim 1 further comprising a first database including the data entity and encryption key identification stored thereon and a second database including the encryption key stored thereon.

13. The computer readable medium according to claim 12 wherein the first database further includes a system key common name stored thereon, and the system key common name corresponds to a system key used to encrypt the encryption key identification.

14. The computer readable medium according to claim 13 further comprising a security token including the system key stored thereon.

15. The computer readable medium according to claim 14 wherein the security token comprises a Smart Card reader.

16. The computer readable medium according to claim 1 wherein the at least one encryption key identification is stored as an attribute of the data entity.

17. The computer readable medium according to claim 1 wherein the data entity comprises a data object having a plurality of attributes.

18. The computer readable medium according to claim 1 further comprising a second data entity including as attributes the encryption key and the encryption key identification.

19. The computer readable medium according to claim 18 wherein the second data entity is stored on a separate isolated database from the at least one data entity.

20. The computer readable medium according to claim 1 further comprising a second data entity encrypted by a second encryption key, the second data entity having a second searchable attribute, and a second encryption key identification corresponding to the second encryption key; and wherein the at least one encryption key comprises a first encryption key and the at least one encryption key identification comprises a first encryption key identification.

21. The computer readable medium according to claim 20 wherein the second encryption key identification is stored as an attribute of the second data entity.

22. The computer readable medium according to claim 20 wherein the first and second encryption key identifications are encrypted by a system key having a system key common name.

23. The computer readable medium according to claim 22 wherein the system key comprises a public system key.

24. The computer readable medium according to claim 22 further comprising the system key common name stored as an attribute of the first and second data entities.

25. The computer readable medium according to claim 20 wherein the first encryption key identification is encrypted by a first system key, and the second encryption key identification is encrypted by a second system key.

26. The computer readable medium according to claim 20 wherein the first and second data entities contain information for an individual customer.

27. The computer readable medium according to claim 26 wherein the first data entity contains medical patient name information, and the second data entity contains medical patient address information.

28. A computer readable data transmission medium containing a data structure for encrypted data, the data structure comprising:

at least one data entity encrypted by at least one encryption key, the data entity having at least one searchable attribute; and

at least one encryption key identification in association with the data entity and corresponding to the encryption key.

29. A computer readable data transmission medium containing a data structure for encrypted data, the data structure comprising:

a plurality of data entities encrypted by at least one encryption key having an encryption key identification; and

at least one system key common name corresponding to a system key operable to encrypt the encryption key identification.

30. A computer readable medium containing a database structure for storage of encrypted data, the database structure comprising:

a plurality of data entities encrypted by at least one encryption key having an encryption key identification; and

at least one system key common name corresponding to a system key operable to encrypt the encryption key identification.

31. The computer readable medium according to claim 30 wherein the data structure further comprises the encryption key identification.

32. The computer readable medium according to claim 31 wherein the encryption key identification is encrypted by the system key.

33. The computer readable medium according to claim 30 wherein the plurality of data entities includes a first data entity encrypted by the at least one encryption key and a second data entity encrypted by a second encryption key, and further comprising a first encryption key identification corresponding to the at least one encryption key, and a second encryption key identification corresponding to the second encryption key.

34. The computer readable medium according to claim 33 wherein the system key common name comprises a first system key common name corresponding to a first system key, and the data structure further comprising the encryption key identification, which is a first encryption key identification, being encrypted by the first system key, and a second system key common name corresponding to a second system key, and wherein the second encryption key identification is encrypted by the second system key.

35. The computer readable medium according to claim 33 wherein the plurality of data entities includes a third data entity encrypted by the a third encryption key, and further comprising a third encryption key identification corresponding to the third encryption key.

36. The computer readable medium according to claim 35 wherein the first, second, and third data entities pertain to an individual with the first data entity containing name information for the individual, the second data entity containing address information for the individual, and the third data entity containing telephone information for the individual.

37. The computer readable medium according to claim 30 wherein the system key common name is hashed.

38. The computer readable medium according to claim 37 further comprising a system key data entity including the system key common name and the system key common name hash value.

39. The computer readable medium according to claim 38 wherein the plurality of data entities are stored on a first database, and the system key data entity is stored on a second database.

40. A method for storage and retrieval of encrypted data, the method comprising:
encrypting a data entity with an encryption key having an encryption key identification;
storing the data entity; and
storing the encryption key identification in association with the data entity.

41. The method according to claim 40 further comprising:
requesting a data manipulation using a searchable attribute;
searching for matches to the searchable attribute;
searching for the encryption key using the encryption key identification; and
decrypting the data entity with the encryption key.

42. The method according to claim 41 wherein requesting the data manipulation comprises requesting a data update of new information, and further comprising encrypting the new information with a second encryption key.

43. The method according to claim 41 wherein requesting the data manipulation comprises requesting an addition of new information, and further comprising encrypting the new information with a second encryption key.

44. The method according to claim 41 wherein requesting the data manipulation comprises requesting viewing of current information, and further comprising encrypting the viewed information with a second encryption key

45. The method according to claim 40 further comprising encrypting the encryption key identification with a system key having a system key common name.

46. The method according to claim 45 further comprising storing the system key in a security token.

47. The method according to claim 45 further comprising:
requesting a data manipulation using a searchable attribute;
searching for matches to the searchable attribute;
searching for the system key using the system key common name;
decrypting the encryption key identification with the system key;
searching for the encryption key using the encryption key identification; and
decrypting the data entity with the encryption key.

48. The method according to claim 45 wherein encrypting the encryption key identification with a system key comprises encrypting the encryption key identification with a system public key.

49. The method according to claim 48 further comprising decrypting the encryption key identification with a system private key.

50. The method according to claim 45 further comprising storing the system key common name in association with the data entity.

51. The method according to claim 45 further comprising checking for expiration of the system key, and upon expiration of the system key, discontinuing use of the system key and generating and using a new system key.

52. The method according to claim 51 further comprising upon expiration of the system key, retaining the system key for decrypting previously encrypted encryption key identifications.

53. The method according to claim 40 further comprising encrypting the encryption key identification with a system key having a system key common name, hashing the system key common name to create a system key common name hash value, and storing the system key common name and system key hash value in association with the data entity.

54. The method according to claim 53 further comprising:
requesting a data manipulation using a searchable attribute;
searching for matches to the searchable attribute;
searching for the system key common name using the system key hash value;
searching for the system key using the system key common name;
decrypting the encryption key identification with the system key;
searching for the encryption key using the encryption key identification; and
decrypting the data entity with the encryption key.

55. The method according to claim 53 further comprising verifying the system key with a private certificate authority, and performing an integrity check on the system key.

56. The method according to claim 40 further comprising checking the encryption key for expiration.

57. The method according to claim 56 further comprising upon expiration of the encryption key, generating a new encryption key having an expiration date, retrieving data entities using the encryption key, decrypting the retrieved data entities with the encryption key, encrypting the retrieved data entities with the new encryption key, storing the retrieved data entities.

58. The method according to claim 40 further comprising hashing searchable attributes of the data entity to determine data entity attribute hash values and storing the data entity hash values in association with the data entity.

59. The method according to claim 58 further comprising:
requesting a data manipulation using a searchable attribute;
hashing the searchable attribute to create a searchable attribute hash value;
searching for matches to the searchable attribute hash value;
searching for the encryption key using the encryption key identification; and
after retrieving the encryption key, decrypting the data entity with the encryption key.

60. The method according to claim 40 further comprising transmitting the data entity over a data transmission line, and wherein encrypting the data entity comprises encrypting only a portion of the data entity in accordance with a business rule.

61. The method according to claim 40 further comprising generating a new encryption key for each user session.

62. The method according to claim 40 further comprising generating a new encryption key for each user action.

63. The method according to claim 40 further comprising retrieving the encryption key from a separate database, and decrypting the data entity with the encryption key.

64. The method according to claim 40 further comprising auditing the encryption key for a desired event.

65. The method according to claim 40 wherein the data entity and encryption key identification are stored in a first database, and further comprising storing the encryption key in a second database.

66. The method according to claim 40 further comprising encrypting the encryption key identification with a system key having a system key common name, and maintaining the system key within a security domain at all times.

67. The method according to claim 40 further comprising:
requesting a data manipulation using a searchable attribute;
searching for matches to the searchable attribute;
searching for the encryption key using the encryption key identification;
performing an integrity check on the encryption key; and
decrypting the data entity with the encryption key.

68. A method for retrieval of encrypted data at rest, the method comprising:
requesting a data manipulation using a searchable attribute;
searching a plurality of data entities for matches to the searchable attribute;
obtaining an encryption key identification from the data entities;
searching for an encryption key using the encryption key identification; and
decrypting the data entities with the encryption key.

69. The method according to claim 68 further comprising:
obtaining a system key common name from the data entities;
searching for the system key using the system key common name;
decrypting the encryption key identification with the system key;

70. A method for storage and retrieval of encrypted data, the method comprising:

encrypting a plurality of data entities with a rotating and dynamic encryption key having an encryption key identification;

storing the data entities; and

creating and rotating to a new encryption key upon occurrence of a desired rotation event.

71. The method according to claim 70 wherein the desired event comprises beginning a new user session.

72. The method according to claim 70 wherein the desired event comprises beginning a new user action.

73. The method according to claim 70 further comprising encrypting the session encryption key identification with a rotating system key having a system key common name.

74. A method for storage and retrieval of encrypted data, the method comprising:

encrypting a first data entity with a first encryption key having a first encryption key identification;

storing the first data entity;

storing the first encryption key identification in association with the first data entity;

encrypting a second data entity with a second encryption key having a second encryption key identification;

storing the second data entity; and

storing the second encryption key identification in association with the second data entity.

75. The method according to claim 74 further comprising encrypting the first and second encryption key identifications with a system key having a system key common name, and storing the system key common name in association with the first and second data entities.

76. The method according to claim 75 wherein the first and second data entities are linked and relate to an individual.

77. The method according to claim 76 further comprising:
requesting a data manipulation using a searchable attribute relating to the individual;
searching for matches to the searchable attribute;
locating the linked first and second data entities relating to the individual;
retrieving the system key common name;
searching for the system key using the system key common name;
decrypting the first and second encryption key identifications with the system key;
searching for the first and second encryption keys using the first and second encryption key identifications;
decrypting the first data entity with the first encryption key; and
decrypting the second data entity with the second encryption key.

78. The method according to claim 74 further comprising encrypting the first encryption key identification with a first system key having a first system key common name, and storing the first system key common name in association with the first data entity, and encrypting the second encryption key identification with a second system key having a second system key common name, and storing the second system key common name in association with the second data entity.

79. The method according to claim 78 further comprising:
requesting a data manipulation using a searchable attribute relating to the individual;
searching for matches to the searchable attribute;
locating the linked first and second data entities relating to the individual;
retrieving the first and second system key common names;
searching for the first and second system keys using the first and second system key common names;
decrypting the first encryption key identification with the first system key;
decrypting the second encryption key identification with the second system key;

searching for the first and second encryption keys using the first and second encryption key identifications;

decrypting the first data entity with the first encryption key; and

decrypting the second data entity with the second encryption key.

80. A computer system comprising:

an encryption key manager operable to generate an encryption key having an encryption key identification, the encryption key being operable to encrypt a data entity; and

an information database operable to store the data entity in an encrypted form and the information database being operable to store the encryption key identification in association with the data entity.

81. The computer system according to claim 80 further comprising a system key manager operable to generate a system key having a system key common name, the system key being operable to encrypt the encryption key identification.

82. The computer system according to claim 81 wherein the information database is further operable to store the system key common name in association with the data entity.

83. The computer system according to claim 81 further comprising a security token and a security token reader operable to receive the security token, and wherein the system key is stored on the security token.

84. The computer system according to claim 83 wherein the security token comprises a Smart Card and the security token reader comprises a Smart Card reader.

85. The computer system according to claim 80 further comprising an encryption key database operable to store the encryption key.

86. The computer system according to claim 85 further comprising a system key manager operable to generate a system key having a system key common name, the system key

manager being further operable to hash the system key common name to create a system key common name hash value, the system key being operable to encrypt the encryption key identification, and a system key database operable to store the system key common name hash value and the system key common name.

87. The computer system according to claim 80 further comprising a hardware random number generator operable to generate the encryption key.

88. The computer system according to claim 80 further comprising a key lifetime manager operable to monitor encryption key expiration dates and request new encryption keys upon expiration of old encryption keys.

89. The computer system according to claim 88 wherein the key lifetime manager is operable to replace the encryption key with the new encryption key.

90. The computer system according to claim 80 wherein the encryption key manager is operable to generate a new encryption key upon the occurrence of a desired event.

91. The computer system according to claim 90 wherein the desired event comprises expiration of the encryption key.

92. The computer system according to claim 90 wherein the desired event comprises beginning a new user action.

93. The computer system according to claim 80 further comprising a system key manager operable to generate a system key having a system key common name, the system key being operable to encrypt the encryption key identification, and a key lifetime manager operable to monitor system key expiration dates and request new system keys upon expiration of old system keys

94. The computer system according to claim 80 further comprising a general security manager operable to communicate with external computer systems, and wherein the encryption key manager is only operable to communicate with the general security manager.

95. The computer system according to claim 80 further comprising a business logic component operable to determine what portions of the data entity are encrypted, and wherein the encryption key manager is not operable to communicate with the business logic component.

96. A computer readable medium containing instructions for controlling a computer system to encrypt and decrypt data, by:
encrypting a data entity with an encryption key having an encryption key identification;
storing the data entity; and
storing the encryption key identification in association with the data entity.

97. The method according to claim 96 further comprising:
requesting a data manipulation using a searchable attribute;
searching for matches to the searchable attribute;
searching for the encryption key using the encryption key identification; and
decrypting the data entity with the encryption key.

98. A method of providing a secure environment for the storage of information, the method comprising:
encrypting a data entity with an encryption key having a randomly generated encryption key identification;
storing the data entity; and
storing the encryption key identification in association with the data entity.

99. The method according to claim 98 further comprising encrypting the encryption key identification with a system key having a system key common name.

100. A method in a computer system for displaying customer information, the method comprising:

receiving a request to view information from a user;

retrieving the information;

checking a security status of the information;

reviewing a security access list to find an identification corresponding to the user;

checking a security access level of the user;

adapting display parameters to modify available display fields based on the security access level of the user;

displaying the permitted information and display fields based on the security access level of the user.

101. The method according to claim 100 wherein adapting the display parameters to modify the available display fields comprises eliminating available display fields corresponding to information the user is not entitled to view.

102. The method according to claim 100 wherein checking the security access level of the user comprises checking a role identification of the user.

103. The method according to claim 100 wherein checking the security access level of the user comprises checking a user identification of the user.

104. The method according to claim 100 further comprising automatically adding to the security access list a responsible user marking the security status of the information as private.

105. A method in a computer system for communicating with an encryption server, the method comprising:

establishing communication with a general security manager of the encryption server;

entering a request for manipulation of data;

receiving a data entity in response to the request;
retrieving security key information from the data entity;
requesting an encryption key;
receiving the encryption key; and
decrypting the data entity.

106. The method according to claim 105 wherein retrieving the security key information from the data entity comprises retrieving an encryption key identification.

107. The method according to claim 105 wherein retrieving the security key information from the data entity comprises retrieving an encryption key identification in an encrypted form and retrieving a system key common name.

108. The method according to claim 105 wherein retrieving the security key information from the data entity comprises retrieving an encryption key identification in an encrypted form and retrieving a system key common name hash value.

109. The method according to claim 105 further comprising receiving a plurality of data entities in response to the request, retrieving security key information from the data entities, requesting multiple encryption keys, and receiving multiple encryption keys.

110. The method according to claim 105 further comprising inserting a security token into a security token reader.

111. An encryption and decryption method for encrypting and decrypting data, the method comprising:
encrypting data with an encryption key having an encryption key identification; and
encrypting the encryption key identification with a system key having a system key common name.

112. The method according to claim 111 further comprising encrypting the encryption key with an encryption key manager digital certificate.

113. The method according to claim 112 further comprising decrypting the encryption key identification with the system key, decrypting the encryption key with an encryption key manager private key corresponding to the encryption key manager digital certificate, and decrypting the data with the encryption key.

114. The method according to claim 113 wherein decrypting data without authorization requires at least copying an information database, copying a key database, and copying a certificate store.

115. The method according to claim 111 further comprising decrypting the encryption key identification with the system key and decrypting the data with the encryption key.

116. The method according to claim 115 wherein decrypting data without authorization requires at least copying an information database, copying a key database, and copying a certificate store.

117. The method according to claim 111 wherein decrypting data occurs only during run time.

118. The method according to claim 111 wherein the encryption key is dynamic and rotating, and the system key is rotating.

119. The method according to claim 111 further comprising encrypting the system key common name and storing the encrypted encryption key identification and encrypted system key common name in association with the data encrypted by the encryption key.

120. The method according to claim 119 wherein encrypting the system key common name comprises hashing the system key common name.